CLAIMS

1. An authenticated device comprising:

a memory unit to store at least one algorithm identifier and at least one encryption key identifier;

a transmitting unit to transmit the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit to an authenticating device;

a receiving unit to receive from the authenticating device a prescribed algorithm identifier and a prescribed encryption key identifier, selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit; and

an authentication processing unit to perform an authentication process with the authenticating device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received by the receiving unit.

2. The authenticated device of claim 1,

wherein the memory unit stores at least one algorithm identifier and at least one encryption key identifier in such a manner that one algorithm identifier and one encryption key identifier are paired as one profile;

wherein the transmitting unit transmits, to the authenticating device, the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit in such a manner that one algorithm identifier and one encryption key identifier are paired as one profile;

wherein the receiving unit receives, from the authenticating device, the prescribed algorithm identifier and the prescribed encryption key identifier paired as a prescribed

profile, among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit; and

wherein the authentication processing unit performs the authentication process with the authenticating device, based on the prescribed algorithm identifier and the prescribed encryption key identifier paired as the prescribed profile received by the receiving unit.

3. The authenticated device of claim 2,

wherein the memory unit further stores a version identifier to identify a version indicating a set in such a manner that one set is formed from at least one algorithm corresponding to the at least one algorithm identifier stored;

wherein the transmitting unit transmits the version identifier stored by the memory unit to the authenticating device;

wherein the receiving unit receives, from the authenticating device, the prescribed algorithm identifier corresponding to a prescribed algorithm among the at least one algorithm forming the set indicated by the version identified by the version identifier transmitted from the transmitting unit; and

wherein the authentication processing unit performs the authentication process with the authenticating device, based on the prescribed algorithm identifier received by the receiving unit and on a prescribed encryption key identifier paired with the prescribed algorithm identifier.

4. An authenticating device comprising:

a memory unit to store at least one algorithm identifier and at least one encryption key identifier;

a receiving unit to receive at least one algorithm identifier and at least one encryption

key identifier from an authenticated device;

a selecting unit to select a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the memory unit from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit, when the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit exist among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit;

a transmitting unit to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting unit to the authenticated device; and

an authentication processing unit to perform an authentication process with the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the transmitting unit.

5. The authenticating device of claim 4,

wherein the memory unit stores at least one profile identifier to identify at least one profile, whereby one algorithm identifier among the at least one algorithm identifier and one encryption key identifier among the at least one encryption key identifier are paired;

wherein the receiving unit further receives at least one profile identifier from the authenticated device;

wherein the selecting unit selects a prescribed profile identifier to be stored by the memory unit from among the at least one profile identifier received by the receiving unit, when the at least one profile identifier stored by the memory unit exists among the at least one profile identifier received by the receiving unit;

wherein the transmitting unit transmits the prescribed profile identifier selected by the selecting unit to the authenticated device; and

wherein the authentication processing unit performs the authentication process with the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier paired by a prescribed profile identified by the prescribed profile identifier transmitted by the transmitting unit.

6. The authenticating device of claim 5,

wherein the memory unit further stores a version identifier to identify a version of a set in such a manner that one set is formed from at least one algorithm corresponding to the at least one algorithm identifier stored;

wherein the receiving unit further receives a prescribed version identifier from the authenticated device;

wherein the selecting unit selects the prescribed algorithm identifier corresponding to one algorithm in the set indicated by the version identified by the prescribed version identifier received by the receiving unit;

wherein the transmitting unit transmits the prescribed algorithm identifier selected by the selecting unit to the authenticated device; and

wherein the authentication processing unit performs the authentication process with the authenticated device, based on the prescribed algorithm identifier transmitted by the transmitting unit and on a prescribed encryption key identifier paired with the prescribed algorithm identifier.

7. An authenticating method comprising:

a first transmitting step to transmit, from an authenticated device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers, to an authenticating device, the plurality of algorithm identifiers and the plurality of encryption key identifiers

stored;

a first receiving step to receive the plurality of algorithm identifiers and the plurality of encryption key identifiers transmitted from the authenticated device by the first transmitting step, at the authenticating device storing at least one algorithm identifier and at least one encryption key identifier;

a selecting step to select, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received by the receiving step, when the at least one algorithm identifier and the at least one encryption key identifier stored by the authenticating device exist among the plurality of algorithm identifiers and the plurality of encryption key identifiers received by the first receiving step;

a second transmitting step to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting step, from the authenticating device to the authenticated device;

a second receiving step to receive the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the second transmitting step, from the authenticating device, at the authenticated device; and

an authentication processing step to perform an authentication process between the authenticating device and the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received by the second receiving step.

8. An authenticating method comprising:

a first transmitting step to transmit, from an authenticated device storing at least one

algorithm identifier and at least one encryption key identifier, to an authenticating device, the at least one algorithm identifier and the at least one encryption key identifier stored;

a first receiving step to receive the at least one algorithm identifier and the at least one encryption key identifier transmitted from the authenticated device by the first transmitting step, at the authenticating device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers;

a selecting step to select, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving step, when at least one of the plurality of algorithm identifiers and at least one of the plurality of encryption key identifiers stored by the authenticating device exist among the at least one algorithm identifier and the at least one encryption key identifier received by the first receiving step;

a second transmitting step to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting step, from the authenticating device to the authenticated device;

a second receiving step to receive the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the second transmitting step, from the authenticating device, at the authenticated device; and

an authentication processing step to perform an authentication process between the authenticating device and the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received by the second receiving step.

9. An authenticating method comprising:

transmitting, from an authenticated device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers, to an authenticating device, the plurality of algorithm identifiers and the plurality of encryption key identifiers stored;

receiving the plurality of algorithm identifiers and the plurality of encryption key identifiers transmitted from the authenticated device, at the authenticating device storing at least one algorithm identifier and at least one encryption key identifier;

selecting, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received, when the at least one algorithm identifier and the at least one encryption key identifier stored by the authenticating device exist among the plurality of algorithm identifiers and the plurality of encryption key identifiers received;

transmitting the prescribed algorithm identifier and the prescribed encryption key identifier selected, from the authenticating device to the authenticated device;

receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted from the authenticating device, at the authenticated device; and

performing an authentication process between the authenticating device and the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received.

10. An authenticating method comprising:

transmitting, from an authenticated device storing at least one algorithm identifier and at least one encryption key identifier, to an authenticating device, the at least one algorithm identifier and the at least one encryption key identifier stored;

receiving the at least one algorithm identifier and the at least one encryption key

identifier transmitted from the authenticated device, at the authenticating device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers;

selecting, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the at least one algorithm identifier and the at least one encryption key identifier received, when at least one of the plurality of algorithm identifiers and at least one of the plurality of encryption key identifiers stored by the authenticating device exist among the at least one algorithm identifier and the at least one encryption key identifier received;

transmitting the prescribed algorithm identifier and the prescribed encryption key identifier selected, from the authenticating device to the authenticated device;

receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted from the authenticating device, at the authenticated device; and

performing an authentication process between the authenticating device and the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received.